Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L1	1101	macro$1 near3 (mov$3 transfer$4 transmit$4 send$3 transmission$1)	USPAT; IBM_TDB	OR	OFF	2005/08/03 11:09
L2	114	macro$1 near3 (copy$3 copies)	USPAT; IBM_TDB	OR	OFF	2005/08/03 11:00
L4	28	l1 and l2	USPAT; IBM_TDB	OR	OFF	2005/08/03 10:35
L5	19	l4 and (flag$3 tag$3 mark$3)	USPAT; IBM_TDB	OR	OFF	2005/08/03 11:00
L6	154236	(macro$1 mov$3 transfer$4 transmit$4 send$3 transmission$1) near3 (global$5 storage$1 memory buffer$1)	USPAT; IBM_TDB	OR	OFF	2005/08/03 10:59
L7	153484	(mov$3 transfer$4 transmit$4 send$3 transmission$1) near3 (global$5 storage$1 memory buffer$1)	USPAT; IBM_TDB	OR	OFF	2005/08/03 11:10
L8	4297	l7 and macro$1	USPAT; IBM_TDB	OR	OFF	2005/08/03 10:59
L9	1511879	l8 (copy$3 copies local$2 document$1 file$1)	USPAT; IBM_TDB	OR	OFF	2005/08/03 11:00
L10	3804	l8 and (copy$3 copies local$2 document$1 file$1)	USPAT; IBM_TDB	OR	OFF	2005/08/03 11:10
L11	344	(flag$3 tag$3 mark$3) near3 macro$1	USPAT; IBM_TDB	OR	OFF	2005/08/03 11:00
L12	100	l10 and l11	USPAT; IBM_TDB	OR	OFF	2005/08/03 11:01
L13	18	l12 and (virus$2 infect$6 abnormal$1 tamper$3)	USPAT; IBM_TDB	OR	OFF	2005/08/03 11:27
L14	94	l1 near3 (global$5 storage$1 memory buffer$1 shared universal$2)	USPAT; IBM_TDB	OR	OFF	2005/08/03 11:10
L15	836	macro$1 near3 (copy$3 copies local$2 document$1 file$1)	USPAT; IBM_TDB	OR	OFF	2005/08/03 11:11
L16	25	l14 and l15	USPAT; IBM_TDB	OR	OFF	2005/08/03 11:14
L17	78	macro$1 near5 (virus$2 infect$6 abnormal$1 tamper$3)	USPAT; IBM_TDB	OR	OFF	2005/08/03 11:13
L18	21	l6 and l17	USPAT; IBM_TDB	OR	OFF	2005/08/03 11:15
L19	9	l15 and l18	USPAT; IBM_TDB	OR	OFF	2005/08/03 11:22

L20	4842	((709/312) or (709/318) or (713/200) or (713/201) or (713/165) or (713/167) or (713/194) or (711/100) or (711/147) or (711/147)).CCLS.	USPAT; IBM_TDB	OR	OFF	2005/08/03 11:26
L21	164	l20 and (macro$1)	USPAT; IBM_TDB	OR	OFF	2005/08/03 11:27
L22	66	l21 and (virus$2 infect$6 abnormal$1 tamper$3)	USPAT; IBM_TDB	OR	OFF	2005/08/03 11:48
L23	27	l22 and l6	USPAT; IBM_TDB	OR	OFF	2005/08/03 11:47
L24	2556	((712/14) or (712/26) or (712/216) or (712/220) or (712/225) or (712/226) or (712/242) or (715/500) or (715/503) or (715/523) or (715/736) or (715/904) or (715/905) or (715/906) or (715/907) or (700/5)).CCLS.	USPAT; IBM_TDB	OR	OFF	2005/08/03 11:48
L25	252	l24 and macro$1	USPAT; IBM_TDB	OR	OFF	2005/08/03 11:48
L26	133	l25 and l6	USPAT; IBM_TDB	OR	OFF	2005/08/03 11:48
L27	2	l26 and (virus$2 infect$6 abnormal$1 tamper$3)	USPAT; IBM_TDB	OR	OFF	2005/08/03 11:48

```
Set     Items   Description
S1      83642   VIRUS? OR TROJAN? OR WORM? OR MALWARE? OR MALICIOUS?(3N)(C-
             ODE? OR PROGRAM? OR MACRO? OR APPLICATION?)
S2     969096   MACRO? OR PROGRAM? OR SCRIPT? OR CODE? OR SOFTWARE?
S3    4326853   MOVE? OR TRANSFER? OR SEND? OR SENT? OR TRANSMIT? OR TRANM-
             IS? OR MOVING?
S4    2051475   RELOCAT? OR TRANSPLANT? OR REMOV? OR EXTRACT? OR EXCIS?
S5     279264   (FIRST OR 1ST OR PRIMARY OR CENTRAL? OR MAIN OR GLOBAL? OR
             MASTER? OR PRINCIPAL? OR PRIME? OR CHIEF?)(7N)(DATABASE? OR D-
             ATA()BASE? OR LOCATION? OR SERVER? OR ENVIRONMENT? OR DOMAIN?
             OR STORAGE? OR WORKSTATION? OR COMPUTER? OR AREA? OR SITE? ? -
             OR ADDRESS?
S6    2896525   COPY? OR COPIE? OR DUPLICAT? OR REPLICA? OR REPRODUC? OR E-
             MULAT? OR MIMIC? OR IMITAT?
S7     285789   (SECOND? OR 2ND OR ANOTHER? OR PARALLEL? OR ADDITIONAL? OR
             BACKUP? OR MULTIP? OR MANY)(7N)(DATABASE? OR DATA()BASE? OR L-
             OCATION? OR SERVER? OR ENVIRONMENT? OR DOMAIN? OR STORAGE? OR
             WORKSTATION? OR COMPUTER? OR AREA? OR SITE? ? OR ADDRESS? OR -
             PLACE?)
S8     259079   FILE? OR DOCUMENT? OR DATAFILE? OR FOLDER? OR DATAFOLDER?
S9     684791   (METHOD? OR SYSTEM? OR PROCESS?? OR PROCEDUR? OR TECHNIQUE?
              OR MODE?)(5N)(DETECT? OR FIND? OR DIAGNOS? OR DETERMIN? OR E-
             VALUAT? OR APPRAIS? OR ASSESS? OR ANALY? OR EXAMIN? OR INSPEC-
             T? OR FLAG? OR QUARANTIN? OR TAG OR TAGS OR TAGGING? OR TAGGE-
             D? OR MARKER?
S10   1530936   IC=(G06F? OR H04L?)
S11     47961   MC=T01-G?
S12    108374   (S1 OR S2) AND S9
S13       426   S12 AND S3:S4(5N)S1:S2 AND S1:S4(5N)S5
S14       212   S12 AND S6(5N)S1:S2 AND (S1:S2 OR S6)(5N)S7:S8
S15        27   S13 AND S1
S16        24   S14 AND S1
S17         3   S13 AND S14
S18       635   S13:S14
S19       137   S18 AND S9/TI AND S1:S2/TI
S20        98   S19 AND S10:S11
S21        52   S15:S17
S22    811720   PR=2000:2005
S23        43   S21 NOT S22
S24        43   IDPAT (sorted in duplicate/non-duplicate order)
S25        78   S20 NOT S21:S22
S26        78   IDPAT (sorted in duplicate/non-duplicate order)
File 347:JAPIO Nov 1976-2005/Apr(Updated 050801)
        (c) 2005 JPO & JAPIO
File 350:Derwent WPIX 1963-2005/UD,UM &UP=200552
        (c) 2005  Thomson Derwent
?
```

24/3,K/28 (Item 28 from file: 350)
DIALOG(R)File 350:Derwent WPIX

012498401 **Image available**
WPI Acc No: 1999-304505/199926
XRPX Acc No: N99-228252
Automatic method for replicating **sufficient samples of computer** virus **for analysis**
Patent Assignee: INT BUSINESS MACHINES CORP (IBMC); IBM CORP (IBMC)
Inventor: BOULAY J Y; PETRILLO A T; SWIMMER M G
Number of Countries: 029 Number of Patents: 008
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week
EP 918285	A2	19990526	EP 98309016	A	19981104	199926 B
JP 11249893	A	19990917	JP 98297935	A	19981020	199949
KR 99044887	A	19990625	KR 9843570	A	19981015	200036
US 6108799	A	20000822	US 9766382	P	19971121	200042
			US 9841493	A	19980312	
JP 3079087	B2	20000821	JP 98297935	A	19981020	200043
TW 445407	A	20010711	TW 98113992	A	19980825	200221
EP 918285	B1	20030326	EP 98309016	A	19981104	200323
DE 69812545	E	20030430	DE 612545	A	19981104	200336
			EP 98309016	A	19981104	

Priority Applications (No Type Date): US 9841493 A 19980312; US 9766382 P 19971121
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
EP 918285	A2	E	16	G06F-011/00	
Designated States (Regional): AL AT BE CH CY DE DK ES FI FR GB GR IE IT LI LT LU LV MC MK NL PT RO SE SI					
JP 11249893	A		19	G06F-009/06	
KR 99044887	A			G06F-015/18	
US 6108799	A			G06F-011/00	Provisional application US 9766382
JP 3079087	B2		19	G06F-009/06	Previous Publ. patent JP 11249893
TW 445407	A			G06F-011/00	
EP 918285	B1	E		G06F-011/00	
Designated States (Regional): DE FR GB					
DE 69812545	E			G06F-011/00	Based on patent EP 918285

RELATED DOC BENEATH

Automatic method for replicating **sufficient samples of computer** virus **for analysis**

Abstract (Basic):
... The **system** for **virus analysis** automatically **replicates** infected **files** . A suspected **virus file** is loaded into a test application, e.g. wordprocessor. Using message passing or/and a **scripting** system, the control system sends commands and simulated keystrokes to the application. The **system determines** if this creates new **files** containing the **virus** . Depending on whether or not the **virus** is polymorphic, differing numbers of samples are generated.
... Automatic computer **virus** sample generation...

...Reduces the effort needed to create **virus copies** including automatically deciding how many replications are needed for analysis...

...The figure shows a logic flow diagram of a global **macro virus replication** process in accordance with the invention...

...Cause **virus** to **replicate** using **scripting** (1.3,1.4,1.6...

...Check if **virus** **files** produced (,1.5,1.7,1.9...
...Title Terms: **VIRUS** ;

```
Set     Items   Description
S1     787851   VIRUS? OR TROJAN? OR WORM? OR MALWARE? OR MALICIOUS?(3N)(C-
             ODE? OR PROGRAM? OR MACRO? OR APPLICATION?)
S2    5520560   MACRO? OR PROGRAM? OR SCRIPT? OR CODE? OR SOFTWARE?
S3    4116534   MOVE? OR TRANSFER? OR SEND? OR SENT? OR TRANSMIT? OR TRANM-
             IS? OR MOVING?
S4    2721161   RELOCAT? OR TRANSPLANT? OR REMOV? OR EXTRACT? OR EXCIS?
S5     611421   (FIRST OR 1ST OR PRIMARY OR CENTRAL? OR MAIN OR GLOBAL? OR
             MASTER? OR PRINCIPAL? OR PRIME? OR CHIEF?)(7N)(DATABASE? OR D-
             ATA()BASE? OR LOCATION? OR SERVER? OR ENVIRONMENT? OR DOMAIN?
             OR STORAGE? OR WORKSTATION? OR COMPUTER? OR AREA? OR SITE? ? -
             OR ADDRESS?
S6    2340807   COPY? OR COPIE? OR DUPLICAT? OR REPLICA? OR REPRODUC? OR E-
             MULAT? OR MIMIC? OR IMITAT?
S7     719112   (SECOND? OR 2ND OR ANOTHER? OR PARALLEL? OR ADDITIONAL? OR
             BACKUP? OR MULTIP? OR MANY)(7N)(DATABASE? OR DATA()BASE? OR L-
             OCATION? OR SERVER? OR ENVIRONMENT? OR DOMAIN? OR STORAGE? OR
             WORKSTATION? OR COMPUTER? OR AREA? OR SITE? ? OR ADDRESS? OR -
             PLACE?)
S8     974090   FILE? OR DOCUMENT? OR DATAFILE? OR FOLDER? OR DATAFOLDER?
S9    6682794   (METHOD? OR SYSTEM? OR PROCESS?? OR PROCEDUR? OR TECHNIQUE?
              OR MODE?)(5N)(DETECT? OR FIND? OR DIAGNOS? OR DETERMIN? OR E-
             VALUAT? OR APPRAIS? OR ASSESS? OR ANALY? OR EXAMIN? OR INSPEC-
             T? OR FLAG? OR QUARANTIN? OR TAG OR TAGS OR TAGGING? OR TAGGE-
             D? OR MARKER?
S10    280683   LOCAL?(7N)(DATABASE? OR DATA()BASE? OR LOCATION? OR SERVER?
              OR ENVIRONMENT? OR DOMAIN? OR STORAGE? OR WORKSTATION? OR CO-
             MPUTER? OR AREA? OR SITE? ? OR ADDRESS? OR PLACE? OR FILE? OR
             DOCUMENT? OR FOLDER? OR DATAFOLDER?)
S11    975369   S1:S2 AND S9
S12      2057   S11 AND S9(7N)S1
S13         6   S12 AND S3:S4(7N)S5
S14         2   S12 AND S6(7N)(S7:S8 OR S10)
S15         8   S13:S14
S16         5   S15 AND PY<2000
S17         4   RD (unique items)
S18      2049   S12 NOT S15
S19      2049   S18 AND (S1 OR MACRO?)
S20        37   S19 AND S3:S4 AND S6
S21       512   S19 AND (S3:S4 OR S6)
S22        35   S21 AND (S5 OR S7:S8 OR S10)
S23        66   S20 OR S22
S24        35   S23 AND PY<2000
S25        31   RD (unique items)
S26    696326   (S1 OR MACRO?) AND (DETECT? OR FIND? OR DIAGNOS? OR DETERM-
             IN? OR EVALUAT? OR APPRAIS? OR ASSESS? OR ANALY? OR EXAMIN? OR
              INSPECT? OR FLAG? OR QUARANTIN? OR TAG OR TAGS OR TAGGING? OR
              TAGGED? OR MARKER? OR IDENTIF? OR ISOLAT? OR CORDON?)
S27     13821   S26 AND (S3:S4 OR S6) AND (S5 OR S7:S8 OR S10)
S28      1636   S27 AND S3:S4 AND S6
S29       120   S28 AND S5 AND (S7:S8 OR S10)
S30       120   S29 NOT (S15 OR S23)
S31        74   S30 AND PY<2000
S32        74   RD (unique items)
S33      4027   S27 AND S1/TI
S34       245   S33 AND (S5 OR S7:S8 OR S10 OR S9)/TI
S35       230   S34 NOT (S29 OR S23 OR S15)
S36       142   S35 AND PY<2000
S37       128   RD (unique items)
File   2:INSPEC 1969-2005/Aug W1
         (c) 2005 Institution of Electrical Engineers
```

```
File   6:NTIS 1964-2005/Aug W1
         (c) 2005 NTIS, Intl Cpyrght All Rights Res
File   8:Ei Compendex(R) 1970-2005/Aug W1
         (c) 2005 Elsevier Eng.  Info. Inc.
File  34:SciSearch(R) Cited Ref Sci 1990-2005/Aug W1
         (c) 2005 Inst for Sci Info
File  35:Dissertation Abs Online 1861-2005/Jul
         (c) 2005 ProQuest Info&Learning
File  65:Inside Conferences 1993-2005/Aug W2
         (c) 2005 BLDSC all rts. reserv.
File  94:JICST-EPlus 1985-2005/Jun W4
         (c)2005 Japan Science and Tech Corp(JST)
File  99:Wilson Appl. Sci & Tech Abs 1983-2005/Jul
         (c) 2005 The HW Wilson Co.
File 111:TGG Natl.Newspaper Index(SM) 1979-2005/Aug 16
         (c) 2005 The Gale Group
File 144:Pascal 1973-2005/Aug W1
         (c) 2005 INIST/CNRS
File 239:Mathsci 1940-2005/Oct
         (c) 2005 American Mathematical Society
File 256:TecInfoSource 82-2005/Jul
         (c) 2005 Info.Sources Inc
?
```

17/3,K/1 (Item 1 from file: 2)
DIALOG(R)File 2:INSPEC

04318649 INSPEC Abstract Number: C9302-6150J-023
Title: Static analysis virus detection **tools for UNIX** systems
Author(s): Kerchen, P.; Lo, R.; Crossley, J.; Elkinbard, G.; Levitt, K.; Olsson, R.
Author Affiliation: Div. of Comput. Sci., California Univ., Davis, CA, USA
Conference Title: 13th National Computer Security Conference. Proceedings. Information Systems Security. Standards - the Key to the Future p.350-65 vol.1
Publisher: NIST, Gaithersburg, MD, USA
Publication Date: 1990 Country of Publication: USA 2 vol. xi+839 pp.
Conference Sponsor: NIST
Conference Date: 1-4 Oct. 1990 Conference Location: Washington, DC, USA
Language: English
Subfile: C

Title: Static analysis virus detection **tools for UNIX** systems
Abstract: The paper proposes two heuristic tools for detecting **viruses** in a UNIX environment. The tools would be used to detect infected **programs** prior to their installation. The tools use static **analysis** and verification **techniques** . One tool, the **detector** , searches for duplication of operating **system** calls. A **program** compiled and linked from source **code** (such as C) makes calls to standard library routines for operating **system** services; relevant to **detecting viruses** are calls on files services, such as open and write. Such object **code** will contain only one instance of the standard library subroutine for each type of service requested by the **program** . A **virus** would most likely carry along its own system calls, hence an infected **program** would have **duplicate** calls to the **file** service and is easily caught by the detector. The second tool, the filter, uses static analysis to determine all of the files which a **program** is capable of writing to. By knowing what files a **program** can and cannot write, one can decide whether or not that **program** is suspicious. The paper discusses the features and shortcomings of both tools and gives some implementation details related to the detection of UNIX **viruses** . In order to defeat these tools, a **virus** would have to be quite complex and, if successful in avoiding detection by these tools, accept limited propagation. The tools are also useful for detecting more general **malicious code** , such as **Trojan** Horses.
...Descriptors: utility **programs**
Identifiers: **virus** detection tools...

... **Trojan** Horses
1990

25/3,K/2 (Item 2 from file: 2)
DIALOG(R)File 2:INSPEC

5621589 INSPEC Abstract Number: C9708-6130S-050
Title: Biologically inspired defenses against computer viruses
Author(s): Kephart, J.O.; Sorkin, G.B.; Arnold, W.C.; Chess, D.M.; Tesauro, G.J.; White, S.R.
Author Affiliation: High Integrity Comput. Lab., IBM Thomas J. Watson Res. Center, Yorktown Heights, NY, USA
Conference Title: IJCAI-95. Proceedings of the Fourteenth International Joint Conference on Artificial Intelligence Part vol.1 p.985-96 vol.1
Editor(s): Mellish, C.S.
Publisher: Morgan Kaufmann Publishers, San Mateo, CA, USA
Publication Date: 1995 Country of Publication: USA 2 vol. (xxx+xiii+2077) pp.
Material Identity Number: XX95-01996
Conference Title: Proceedings of International Joint Conference on Artificial Intelligence
Conference Sponsor: Int. Joint Conferences on Artificial Intelligence; American Assoc. Artificial Intelligence; Canadian Soc. Computational Studies of Intelligence; Soc. Canadienne pour l'etude de l'intelligence par ordinateur
Conference Date: 20-25 Aug. 1995 Conference Location: Montreal, Que., Canada
Language: English
Subfile: C

Title: Biologically inspired defenses against computer viruses
Abstract: Today's anti- **virus** technology, based largely on analysis of existing **viruses** by human experts, is just barely able to keep pace with the more than three new computer **viruses** that are written daily. In a few years, intelligent agents navigating through highly connected networks are likely to form an extremely fertile medium for a new breed of **viruses** . At IBM, we are developing novel, biologically inspired anti- **virus** techniques designed to thwart both today's and tomorrow's **viruses** . We describe two of these: a neural network **virus** detector that learns to discriminate between infected and uninfected **programs** , and a computer immune **system** that **identifies** new **viruses** , **analyzes** them automatically, and uses the results of its analysis to detect and **remove** all **copies** of the **virus** that are present in the system. The neural-net technology has been incorporated into IBM's commercial anti- **virus** product; the computer immune system is in prototype.
Descriptors: computer **viruses** ;
Identifiers: computer **viruses** ; ...
...anti- **virus** technology...

...neural network **virus** detector
1995

25/3,K/3 (Item 1 from file: 6)
DIALOG(R)File 6:NTIS

1987447 NTIS Accession Number: PB97-852446
Computer Viruses : Identification , Mode **of Infection, and Protection. (Latest citations from the INSPEC Database)**
(Published Search)
NERAC, Inc., Tolland, CT.
Corp. Source Codes: 103588000
Sponsor: National Technical Information Service, Springfield, VA.
Dec 96 50-250 citations
Languages: English Document Type: Bibliography
Journal Announcement: GRAI9705
Updated with each order. Supersedes PB96-851217. Sponsored in part by National Technical Information Service, Springfield, VA.
Order this product from NTIS by: phone at 1-800-553-NTIS (U.S. customers); (703)605-6000 (other countries); fax at (703)321-8547; and email at orders@ntis.fedworld.gov. NTIS is located at 5285 Port Royal Road, Springfield, VA, 22161, USA.
NTIS Prices: PC N01/MF N01

Computer Viruses : Identification , Mode **of Infection, and Protection. (Latest citations from the INSPEC Database)**
The bibliography contains citations concerning computer **viruses** . These small, secretly introduced **programs** can destroy data or hardware, although most to date have inserted humorous or annoying messages on existing **programs** . Bulletin boards, online systems, shared **software** , **local area** networks, and dealer-demonstrated **software** are among the potential sources of **virus** infections discussed. Topics include internal **virus** protection **programs** , security systems, and **virus** protection **software** . Legal liability for **virus** introduction is **examined** . Ridding a computer **system** of a known **virus** is briefly considered. **Methods** of **virus identification** and specific computer **viruses** are examined.(Contains 50-250 citations and includes a subject term index and title list.) (**Copyright** NERAC, Inc. 1995)
Descriptors: *Bibliographies; *Data processing security; *Electronic security; *Data encryption; Computer **software** ; Cryptology
Identifiers: *Computer **viruses** ; *Secure communications; *Computer security; Published Searches; Computer information security; Computer privacy; NTISNTISH; NTISNERACD

32/3,K/74 **(Item 1 from file: 256)**
DIALOG(R)File 256:TecInfoSource

00115910 DOCUMENT TYPE: Review

PRODUCT NAMES: Viruses **&** Worms **(838942); E-Mail (830031**

TITLE: Melissa Virus **Portends Bigger Security Risks**
AUTHOR: Carr, David F Luh, James C
SOURCE: Internet World, v5 n13 p7(1) Apr 5, 1999
ISSN: 1097-8291
HOMEPAGE: http://www.iw.com

RECORD TYPE: Review
REVIEW TYPE: Product Analysis
GRADE: Product Analysis, No Rating

REVISION DATE: 20030930

PRODUCT NAMES: Viruses **&** Worms **(**

TITLE: Melissa Virus **Portends Bigger Security Risks**

Another e-mail **virus** has been discovered that uses Microsoft Office **macros** to first infect a Word default **document** template, then each ensuing Word **document** created from the default template. Called Melissa, the **virus** also spreads to a user's Microsoft Outlook e-mail program and automatically **sends** itself as a legitimate Word **file** attachment to the **first** 50 **address** book contacts. Melissa then spreads itself into the e-mail recipient's hard drive when the user opens the Word attachment, in order to **replicate** itself further. Though Melissa incurs a minimum amount of damage compared to many other **viruses** , the fact it can so easily infect millions of e-mail users around the world has **analysts** worried about future **viruses** that may be less playful. Even more disturbing is that the Melissa **virus** code takes up less than a page of code. Melissa's simplicity could thus encourage other more violent hackers to create more destructive **viruses** .

DESCRIPTORS: E-Mail; Microsoft Word; Office Suites; **Viruses** & **Worms**
1999

37/3,K/2 (Item 2 from file: 2)
DIALOG(R)File 2:INSPEC

5302473 INSPEC Abstract Number: C9608-6130S-009
Title: Global **behaviour of** computer virus **diffusion and extinction**
Author(s): Sengoku, Y.; Okamoto, E.; Mambo, M.; Uyematsu, T.
Author Affiliation: Sch. of Inf. Sci., Japan Adv. Inst. of Sci. & Technol., Japan
Journal: Transactions of the Information Processing Society of Japan vol.37, no.4 p.579-87
Publisher: Inf. Process. Soc. Japan,
Publication Date: April 1996 Country of Publication: Japan
CODEN: JSGRD5 ISSN: 0387-5806
SICI: 0387-5806(199604)37:4L.579:GBCV;1-U
Material Identity Number: T205-96007
Language: Japanese
Subfile: C

Title: Global **behaviour of** computer virus **diffusion and extinction**
Abstract: We **analyze** both in theory and by simulation the spread of computer **viruses** in a network composed of personal computers, and show there is the relation between **virus** diffusion and graphic properties of a network, i.e., the diameter and the average distance. By introducing the infection rate of the **virus** and the extermination rate by vaccine, we obtain the extermination rate for completely **removing viruses** from a network under each infection rate. From these results we discuss further what kind of network lessens the **virus** diffusion.
Descriptors: computer **viruses** ; ...

... **local area** networks
Identifiers: computer **virus** diffusion...

...computer **virus** extinction...

... **virus** infection rate...

... **local area** networks
1996

37/3,K/4 (Item 4 from file: 2)
DIALOG(R)File 2:INSPEC

4629106 INSPEC Abstract Number: C9405-6130S-004
Title: A method **of** detecting **and eradicating known and unknown** viruses **(PC** viruses **)**
Author(s): Mostovoy, D.Yu.
Author Affiliation: DialogueScience Inc., Moscow, Russia
Journal: IFIP Transactions A (Computer Science and Technology) vol.A-43 p.109-12
Publication Date: 1994 Country of Publication: Netherlands
CODEN: ITATEC ISSN: 0926-5473
Conference Title: Security and Control of Information Technology in Society. IFIP TC9/WG9.6 Working Conference
Conference Date: 12-17 Aug. 1993 Conference Location: St. Petersburg, Russia
Language: English
Subfile: C

Title: A method **of** detecting **and eradicating known and unknown** viruses **(PC** viruses **)**
Abstract: First, **virus detection** and **removal** methods which **identify** and **remove** almost all of the as-yet-unknown **file** and boot infectors are outlined. These methods are then shown to be implemented in the...
Descriptors: computer **viruses**
Identifiers: PC **viruses** ; ...

... **virus detection** ; ...

... **file** infectors
1994